UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/752,385	01/06/2004	Hashem M. Ebrahimi	1565.066US1	6809

21186 7590 11/04/2008

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
11/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/752,385	EBRAHIMI ET AL.	
	Examiner	Art Unit	
	CANH LE	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 August 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,6,8,10 and 12-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,6,8,10 and 12-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the communication filed on 08/27/2008.

Claims 3-5, 7, 9, 11, and 22-30 have been cancelled.

Claims 1, 8, and 16 have been amended.

Claims 1-2, 6, 8, 10, 12-21 have been examined and are pending.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/27/2008 has been entered.

Response to Arguments

Applicant's arguments filed 07/30/2008 have been fully considered but they are not persuasive. The Applicant argues the following:

(A) Subramaniam does not disclose "inspecting the content within a secure site".

The Examiner respectfully disagrees with the Applicant as the following reasons:

Per (A):

Subramaniam teaches inspecting the content within a secure site *[Subramaniam : Col. 5; lines 25-27; "The secure network 100 includes one or more file or object or Web servers such as target server 104"; figs. 1, 3; The target server 104 is in the secure network 100; Col. 10, lines 59-66; "The target server 104 can then transform any non-secure data 130 to the border server 106 for subsequent transmission to the external client 112."].*

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 6, 8, 13, and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Subramaniam** et al. (US Patent: 6,081,900).

As per claim 1:

Subramaniam discloses a method to manage secure communications, comprising:

(a) establishing a secure session on a secure site with an external client that communicates from an insecure site **[Subramaniam : Col. 3 lines 35-50; Col. 3, line 66 to Col. 4 line 17];**

(b) detecting access attempts during the session directed to insecure transactions, the insecure transactions identified as links to a site **[Subramaniam : Col. 6, lines 40-60; By**

checking the IP address which the request was made, the target server 104 determines that the request came from outside the security parameter 102. The target server 104 check user permission against access control list associated with the data"; fig. 1, Border server 106 includes URL transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; "The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links, URLs, or other references which, if presented by the external client 112 to the secure network 100, ...which contain URLs specifying "http://" rather than "https://" in reference to data stored on the target server 104 are examples of non-secure data 130"; Col. 10, lines 10-19]; and

(c) transparently managing the access attempts by pre-acquiring content from the secure site by accessing the links on behalf of the client to pre-acquire the content and by scanning and inspecting the content within the secure site before determining whether the content should be made available to the external client during the secure session **[Subramaniam : Col. 6, lines 40-60; The target server 104 check user permission against access control list associated with the data, or take other steps to make sure the requesting user is entitled to access the request data before providing data"; fig. 1, Border server 106 includes URL transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; "The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links, URLs, or other references which, if**

presented by the external client 112 to the secure network 100, ….which contain URLs specifying "http://" rather than "https://" in reference to data stored on the target server 104 are examples of non-secure data 130"; Col. 10, lines 10-19; Col. 5; lines 25-27; "The secure network 100 includes one or more file or object or Web servers such as target server 104"; figs. 1, 3; The target server 104 is in the secure network 100; Col. 10, lines 59-66; "The target server 104 can then transform any non-secure data 130 to the border server 106 for subsequent transmission to the external client 112."] .

Subramaniam does not explicitly teach wherein the border server is external from the secure site.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to move the border server to an site external from the secure location, since it has been held that it requires routine skill in the art to rearrange the location of the border server because it would not have modified the operation of the device **[See MPEP 2144.04; see also *In re Japikse,* 181 F.2d 1019, 86 USPQ 70 (CCPA 1950)].**

As per claim 2:

Subramaniam further discloses the method of claim 1 wherein the detecting further includes translating non-secure links into secure links for the insecure transactions before presenting results of the access attempts to the external client **[Subramaniam : Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)].**

As per claim 6:

Subramaniam discloses the method of claim 1 wherein managing further includes at least one or more of: issuing alerts **[Subramaniam : Col. 11, lines 61-67]**, notifications **[Subramaniam : Col. 8, lines 40-57],** or advisories to a monitoring entity or log.

As per claim 8:

Subramaniam discloses a method to manage secure communications, comprising:

(a) detecting insecure transactions occurring during a secure session, wherein the insecure transactions result from actions requested by an external client participating in the secure session **[Subramaniam : Col. 6, lines 40-60; By checking the IP address which the request was made, the target server 104 determines that the request came from outside the security parameter 102];**

(b) inspecting the insecure transactions in advance of satisfying the actions requested by pre-acquiring content associated with the insecure transactions before making available to the external client , and wherein the insecure transactions are associated with links to an site, and wherein content are pre-acquired from the site via the links and inspected and scanned on behalf of the client within a secure site associated with the secure session **[Subramaniam : Col. 6, lines 46-60; A target server check user permissions against access control lists; fig. 1, Border server 106 includes URL transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; "The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links,**

URLs, or other references which, if presented by the external client 112 to the secure network 100, ….which contain URLs specifying "http://" rather than "https://" in reference to data stored on the target server 104 are examples of non-secure data 130"; Col. 10, lines 10-19; figs. 1, 3; The target server 104 is in the secure network 100; Col. 10, lines 59-66; "The target server 104 can then transform any non-secure data 130 to the border server 106 for subsequent transmission to the external client 112."]; and

making a determination in response to the inspection for at least one of the following: permitting the insecure transactions to proceed unmodified by performing the actions requested for the external client, permitting the insecure transactions to proceed in a modified fashion **[Subramaniam : Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)],** and denying the insecure transactions by denying the actions requested.

Subramaniam does not explicitly teach wherein the border server is external from the secure site.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to move the border server to an site external from the secure location, since it has been held that it requires routine skill in the art to rearrange the location of the border server because it would not have modified the operation of the device **[See MPEP 2144.04; see also *In re Japikse,* 181 F.2d 1019, 86 USPQ 70 (CCPA 1950)].**

As per claim 13:

Subramaniam further discloses the method of claim 8 wherein the making a determination further includes permitting the insecure transactions to proceed in a modified fashion by transparently processing the external client access attempt within a proxy making the external client access attempt appear to be part of the secure session **[Subramaniam : Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)].**

As per claim 16:

This claim has limitations that are similar to those of claims 1 and 8, thus it is rejected with the same rationale applied against claims 1 and 8 above.

As per claim 17:

Subramaniam further discloses the secure communications management system of claim 16 wherein the secure communications manager translates Hypertext Transfer Protocol (HTTP) insecure communications into HTTP over Secure Sockets Layer (HTTPS) secure communications during the secure session **[Subramaniam : Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)].**

Claims 10, 12, 14-15, and 18-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Subramaniam** et al. (US Patent: 6,081,900) in view of "Netscape Proxy Server Administrator's Guide Version 3.5 for Unix", 1997, as provided by applicant herein after **Netscape_unix_v3.5.**

As per claim 10:

Subramaniam further discloses a method permitting the insecure transactions to proceed in the modified fashion by changing the reference links from Hypertext Transfer Protocol (HTTP) insecure links to HTTP over Secure Sockets Layer (HTTPS) **[Subramaniam : Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)].**

Subramaniam does not explicitly disclose to suppress the security warning messages. Netscape_unix_v3.5 discloses to suppress the security warning messages **[Chapter 10, pages 1-3; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be an empty text].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improve techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated **[the background of this application].**

As per claim 12:

Subramaniam discloses the method as described in claim 8.

Subramaniam does not disclose a method permitting insecure transactions to proceed unmodified.

The background of the invention discloses a method permitting insecure transactions to proceed unmodified **[Col. 2, lines 36-41].**

Subramaniam and the background of the invention do not disclose permitting normally occurring security warnings to be presented to the client before satisfying the external client access attempt to reference the external site.

Netscape_unix_v3.5 discloses permitting normally occurring security warnings to be presented to external the client before satisfying the external client access attempt to reference the external site **[Chapter 10, pages 1-3; Chapter 13, page 1; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be security warning messages].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify Subramaniam and the method of the background of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated **[the background of this application].**

As per claim 14:

Subramaniam discloses the method as described in claim 8.

Subramaniam does not disclose a method as described in claim 14.

Netscape_unix_v3.5 discloses the method wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and notifying the external client of the denial **[Chapter 13, page 1; A proxy will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated **[the background of this application].**

As per claim 15:

Subramaniam discloses the method as described in claim 8.

Subramaniam does not disclose a method as described in claim 15.

Netscape_unix_v3.5 further discloses the method wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and logging information about the external client access attempt **[Chapter 13, pages 1-7].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure

communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated **[the background of this application].**

As per claim 18:

Subramaniam further discloses the secure communications management system of claim 16 wherein the proxy selectively modifies a number of the insecure communications **[Col. 3, lines 34-51; Col. 3, line 66 to Col. 4, line 8].**

Subramaniam does not explicitly disclose to suppress normally occurring security warning messages that the secure communications manager issues.

Netscape_unix_v3.5 discloses to suppress normally occurring security warning messages that the secure communications manager issues **[Chapter 13, page 1; A proxy will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated **[the background of this application].**

As per claim 19:

The background of the invention discloses the secure communications management system of claim 16 wherein the proxy selectively leaves a number of the insecure communications unchanged **[Col. 2, lines 36-41].**

The background of the invention does not disclose to issue security warning messages to the external client.

Netscape_unix_v3.5 discloses a proxy sending security warning messages to the external client **[Chapter 10, pages 1-3; Chapter 13, page 1; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be security warning messages].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of the background of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated **[the background of this application].**

As per claim 20:

Subramaniam discloses the secure communication system as claimed in claim 16.

Subramaniam does not disclose a proxy which selectively denies a number of the insecure communications to proceed and at performs at least one of reports the denial to another entity and records the denial in a log.

Netscape_unix_v3.5 discloses a proxy which selectively denies a number of the insecure communications to proceed and at performs at least one of reports the denial to another entity and records the denial in a log **[Chapter 13, page 1; A proxy will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt; Proxy error log messages include Catastrophe error, Failure, information log entry, warning flags, and security warning].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated **[the background of this application].**

As per claim 21:

Subramaniam discloses the secure communication system as claimed in claim 16.

Subramaniam does not explicitly disclose a proxy selectively sending custom warning messages or explanations to the external client regarding a number of the insecure communications.

Netscape_unix_v3.5 discloses a proxy which selectively issues custom warning messages or explanations to the external client regarding a number of the insecure communications **[Chapter 10, pages 1-3; Chapter 13, page 1; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be security warning messages].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Subramanian of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated **[the background of this application].**

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zand Kambiz can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Canh Le/

Examiner, Art Unit 2439

October 26, 2008

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434